#6

Substitute Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney's Docket No. 10454-014002	Application No. 09/711,323
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Valdes, et al.	
		Filing Date November 9, 2000	Group Art Unit

U.S. Patent Documents

Examiner Initial	Desig. ID	Patent Number	Issue Date	Patentee	Class	Subclass	Filing Date If Appropriate
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						

Foreign Patent Documents or Published Foreign Patent Applications

Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No
AM	AL	WO 00/34867	15 June 2000	WIPO				
	AM							
	AN							
	AO							
	AP							

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
AM	AQ	Debar, et al., "A Neural network Component for an Intrusion Detection System," 1992 IEEE
AM	AR	Debar et al., "Towards a Taxonomy of Intrusion-Detection Systems," Computer Networks 31 (1999), 805-822
AM	AS	Denning et al., "Requirements and Model for IDES—A Real-Time Intrusion-Detection Expert System," SRI Project 6169, SRI International, Menlo Park, CA, August 1985
AM	AT	Denning, "An Intrusion-Detection Model," SRI International, Menlo Park, CA, Technical Report CSL-149, November 1985
AM	AU	Garvey et al., "An Inference Technique for Integrating Knowledge from Disparate Sources," Proc. IJCAI< Vancouver, B.C., August, 1981, 319-325

Examiner Signature	Date Considered
	4/8/04

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

#6

Substitute Form PTO-1449 (Modified)	U.S. Department of Commerce Patent and Trademark Office	Attorney's Docket No. 10454-014002	Application No. 09/711,323
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		Applicant Valdes, et al.	
		Filing Date November 9, 2000	Group Art Unit

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
AM	AV	Garvey et al., "Model-Based Intrusion Detection," Proceedings of the 14th National Computer Security Conference, Washington DC, October 1991
AM	AW	Goan, "A Cop On the Beat: Collecting and Appraising Intrusive Evidence," Communications of the ACM volume 42 number 7, pp. 46-52
AM	AX	Internet Security Systems Technology Brief, "Intrusion Detection for the Millennium"
AM	AY	Lunt, "A Survey of Intrusion Detection Techniques," Computers & Security, 12 (1993) 405-418
AM	AZ	Lunt, "Automated Audit Trail Analysis and Intrusion Detection: A Survey," Proceedings of the 11th National Computer Security Conference, Baltimore, MD, October 1988
AM	AAA	Judea Pearl, Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference, Morgan Kaufmann Publishers, 1988.
AM	ABB	Xavier Boyen and Daphne Koller, "Tractable Inference for Complex Stochastic Processes," Proceedings of the Fourteenth Annual Conference on Uncertainty in Artificial Intelligence (UAI-98), pp. 33-42, Madison, WI July 24-26, 1988.
AM	ACC	Joint SRI International and Stanford University Proposal EMU 98-79, "Adaptive Model-Based Monitoring and Thread Detection".

Examiner Signature	Date Considered
Anil Mathew	4/8/2004

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

U.S. Department of Commerce, Patent and Trademark Office	Docket No.	Serial No.
(PTO Form 1449 modified)	SRI/4190-3	09/711,323
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Applicant de Jesus Valdes, et al.	Confirmation No.: 6879
(Use several sheets if necessary)	Filing Date November 9, 2000	Group 2161
Examiner		

U.S. Patent Documents

*Examiner Initial		Document Number	Issue Date	Applicant(s), Name	Class	Subclass	Filing Date If Appropriate
AM	A1	6,453,346 B1	09/17/2002	Garg et al.	709	224	
	A2						

Foreign Patent Documents

*Examiner Initial		Document Number	Date	Country	Class	Subclass	Translation Yes	Translation No
	B1						☐	☐

OTHER ART

*Examiner Initial		Including Author, Title, Date, Pertinent Pages, Etc.
AM	C1	Hartley, B., "Intrusion Detection Systems: What You Need to Know," Business Security Advisor Magazine, Doc # 05257, allegedly dated September 1998, http://advisor.com/doc/05257, 7 pages, printed June 10, 2003
AM	C2	Hurwicz, M., "Cracker Tracking: Tighter Security with Intrusion Detection," BYTE.com, allegedly dated May 1998, http://www.byte.com/art/9805/sec20/art1.htm, 8 pages, printed June 10, 2003
AM	C3	"Networkers, Intrusion Detection and Scanning with Active Audit," Session 1305, ©1998Cisco Systems, http://www.cisco.com/networkers/nw99_pres/1305.pdf, 0893-04F9_c3.scr, printed June 10, 2003
AM	C4	Paller, A., "About the SHADOW Intrusion Detection System" Linux Weekly News, allegedly dated September 1998, http://lwn.net/1998/0910/shadow.html, 38 pages, printed June 10, 2003
AM	C5	Cisco Secure Intrusion Detection System, Release 2.1.1, NetRanger User's Guide, Version 2.1.1, © 1998, Cisco Systems, Inc., allegedly released on April 1998, http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids3/index.htm, printed June 10, 2003, 334 pages, (See CSI document listed at C7 below)
AM	C6	Cisco Secure Intrusion Detection System 2.1.1 Release Notes, Table of Contents, Release Notes for NetRanger 2.1.1, © 1992-2002, Cisco Systems, Inc., , allegedly posted September 28, 2002, 29 pages, http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids3/nr11new.htm, printed June 10, 2003
AM	C7	R. Power, et al., "CSI Intrusion Detection System Resource", allegedly dated July 1998, http://216.239.57.100/search?q=cache:gvTCojxD6nMJ:www.gocsi.com/ques.htm+site:www.gocsi.com+ques&hl=en&ie=UTF-8, printed June 16, 2003.

Examiner	Date Considered 9/8/04

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with your communication to applicant.

U.S. Department of Commerce, Patent and Trademark Office	Docket No.	Serial No.
(PTO Form 1449 modified)	SRI/4190-3	09/711,323
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Applicant(s) de Jesus Valdes, et al.	Confirmation No. 5879
(Use several sheets if necessary)	Filing Date	Group
Examiner	November 9, 2000	2161

U.S. Patent Documents

*Examiner Initial		Document Number	Issue Date	Applicant(s) Name	Class	Subclass	Filing Date If Appropriate
	A1	4,672,609	06/1987	Humphrey et al	371	21	
	A2	4,773,028	09/1988	Tallman	364	550	
	A3	5,210,704	05/1993	Husseiny	364	551.01	
	A4	5,440,723	08/08/1995	Arnold et al.	395	181	
	A5	5,539,659	07/1996	McKee, et al.	709	224	
	A6	5,557,742	09/1996	Smaha et al.	395	186	
	A7	5,706,210	01/1998	Kumano et al	709	224	
	A8	5,748,098	05/05/1998	Grace	340	825.16	
	A9	5,790,799	08/1998	Mogul	709	224	
	A10	5,878,420	03/02/1999	De la Salle	707	10	
	A11	5,919,258	07/06/1999	Kayashima et al.	713	201	
	A12	5,922,051	07/13/1999	Sidey	709	223	
	A13	5,940,591	08/17/1999	Boyle, et al.	395	187.01	
	A14	5,974,237	10/1999	Shurmer et al.	709	224	
	A15	5,974,457	10/26/1999	Waclawshy et al	709	224	
	A16	5,991,881	11/23/1999	Conklin et al	713	201	
	A17	6,009,467	12/1999	Ratcliff et al.	709	224	
	A18	6,052,709	04/18/2000	Paul	709	202	
	A19	6,070,244	05/30/2000	Orchier et al.	713	201	
	A20	6,144,961	11/07/2000	De la Salle	707	10	
	A21	6,396,845	05/28/2002	Sugita	370	449	
	A22	6,460,141	10/01/2002	Olden	712	201	
	A23	6,519,703	02/11/2003	Joyce	713	201	
	A24	2002/0032717	03/14/2002	Malan et al.	709	105	05/15/2001
	A25	2002/0032793	03/14/2002	Malan et al.	709	232	05/15/2001
	A26	2002/0035698	03/21/2002	Malan et al.	713	201	05/15/2001
	A27	2002/0032880	03/14/2002	Poletto et al.	714	4	08/16/2001

U.S. Department of Commerce, Patent and Trademark Office	Docket No. SRI/4190-3	Serial No. 09/711,323
(PTO-Form 1449 modified)		
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Applicant de Jesus Valdes, et al.	Confirmation No. 9879
(Use several sheets if necessary)	Filing Date November 9, 2000	Group 2161
Examiner		

	A28	2002/0144156	10/03/2002	Copeland, III	713	201	01/31/2002
	A29	2002/0138753	09/26/2002	Munson	713	200	03/15/2002
	A30	2003/0037136	02/20/2003	Labovitz et al.	709	224	06/27/2002

Foreign Patent Documents

*Examiner Initial		Document Number	Date	Country	Class	Subclass	Translation YES	Translation NO
	B1	99/13427	03/18/1999	WIPO	G06K	7/00	☐	☐
	B2	99/57626	11/11/1999	WIPO	G06F	1/16	☐	☐
	B3	00/10278	02/24/2000	WIPO	H04L		☐	☐
	B4	00/25214	05/04/2000	WIPO	G06F	12/14	☐	☐
	B5	00/25527	05/04/2000	WIPO	H04Q	3/00	☐	☐
	B6	00/34867	06/15/2000	WIPO	G06F	11/30	☐	☐
	B7	02/101516	12/19/2002	WIPO	G06F		☐	☐
	B8						☐	☐

OTHER ART

*Examiner Initial		Including Author, Title, Date, Pertinent Pages, Etc.
	C1	Copeland, J., "Observing Network Traffic - Techniques to Sort Out the Good, the Bad, and the Ugly," http://www.csc.gatech.edu/~copeland/8843/slides/Analyst-011027.ppt, allegedly 2001
	C2	Denning et al, "Prototype IDES: A Real-Time Intrusion-Detection Expert System," SRI Project ECU 7508, SRI International, Menlo Park, California, Aug. 1987
	C3	Dowell, "The Computerwatch Data Reduction Tool," AT&T Bell Laboratories, Whippany, New Jersey.
	C4	Farshchi, J., "Intrusion Detection FAQ, Statistical based approach to Intrusion Detection," http://www.sans.org/resources/idfaq/statistic_ids.php, date unknown, printed 7/10/2003
	C5	Fox, et al., "A Neural Network Approach Towards Intrusion Detection," Harris Corporation, Government Information Systems Division, Melbourne, FL, Jul. 2, 1990.
	C6	Heberlein, et al., "A Network Security Monitor," Proceedings of the IEEE Symposium on Security and Privacy, May 07-09 1990, Oakland, CA, pp 296-304, IEEE Press.
	C7	Ilgun et al., State Transition Analysis: A Rule-Based Intrusion Detection Approach, IEEE Transactions on Software Engineering, vol., 21, No. 3, Mar. 1995
	C8	Jackson, et al., "An Expert System Application For Network Intrusion Detection," Proceedings of the 14th National Computer Security Conference, Washington, DC, 1-4 October 1991.

U.S. Department of Commerce, Patent and Trademark Office	Docket No.	Serial No.
(PTO-Form 1449 modified)	SRI/4190-3	09/711,323
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Applicant de Jesus Valdes et al.	Confirmation No.: 6879
(Use several sheets if necessary)	Filing Date	Group
Examiner	November 9, 2000	2161

	C9	Javitz et al., "The NIDES Statistical Component Description and Justification, SRI International Annual Report A010," Mar. 7, 1994.
	C10	Javitz et al., "The SRI IDES Statistical Anomaly Detector," Proceedings of the IEEE Symposium on Security and Privacy, Oakland,CA, May 1991. pp 316-326, IEEE Press.
	C11	Kaven, "The Digital Dorman," PC Magazine, Nov. 16, 1999.
	C12	Lankewicz, et al., "Real-time Anomaly Detection Using a Nonparametric Pattern Recognition Approach", Proceedings of the 7th Annual Computer Security Applications Conference, San Antonio, Texas, 1991, IEEE Press.
	C13	Liepins, et al., "Anomaly Detection; Purpose and Framework," In Proceedings of the 12th National Computer Security Conference, pages 495-504, October 1989.
	C14	Lindquist, et al., "Detecting Computer and Network Misuse Through the Production-Based Expert System Toolset (P-BEST)," Oct. 25, 1998
	C15	Lippmann, et al., "Evaluating Intrusion Detection Systems: The 1998 DARPA Off-line Intrusion Detection Evaluation," Proceedings of the 2000 DARPA, Information Survivability Conference and Exposition, January 25-27 2000, Hilton Head, SC, Volume 2, pp 1012-1035, IEEE Press.
	C16	Lunt et al., "A Prototype Real-Time Intrusion-Detection Expert System," Proceedings of the 1988 IEEE Symposium on Security and Privacy, Apr. 1988.
	C17	Lunt et al., "An Expert System to Classify and Sanitize Text", Proceedings of the 3rd Aerospace Computer Security Conference, December 7-11 1987, pp 30-34
	C18	Lunt et al., "Knowledge-Based Intrusion Detection", Proceedings of the AI Systems in Government Conference, Washington DC, March 1989.
	C19	Miller, L., "A Network Under Attack, Leverage Your Existing Instrumentation to Recognize and Respond to Hacker Attacks," http://www.netscout.com/files/Intrusion_020118.pdf, Date Unknown, pg 1-8
	C20	Munson, et al., "Watcher: The Missing Piece of the Security Puzzle," Proceedings of the 17th Annual Computer Security Applications Conference (ACSAC'01), December 10-14 2001, New Orleans, LA, pp 230-239, IEEE Press.
	C21	NetScreen, Products FAQ, http://www.netscreen.com/products/faq.html, Date Unknown
	C22	Porras, et al., "Live Traffic Analysis of TCP/IP Gateways," Proc. 1998 ISOC Symp. On Network and Distributed Systems Security, December 12, 1997, 1-13
	C23	Porras et al, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," 20th NISSC – October 9, 1997.
	C24	Sebring et al., "Expert systems in intrusion detection: A case study". In Proceedings of the 11th National Computer Security Conference, pages 74-81, October 1988.
	C25	Shieh et al., "A Pattern-Oriented Intrusion-Detection Model and Its Application," © 1991 IEEE

U.S. Department of Commerce, Patent and Trademark Office	Docket No.	Serial No.
(PTO/Form 1449 modified)	SRI/4190-3	09/711,323
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Applicant de Jesus Valdes, et al.	Confirmation No.: 6879
(Use several sheets if necessary)	Filing Date November 9, 2000	Group 2161
Examiner		

	C26	Skinner, "EMERALD TCP Statistical Analyzer 1998 Evaluation Results," http://www.sdl.sri.com/emerald/98-eval-estat/index.html, Allegedly dated July 9, 1999
	C27	Smaha, "Haystack: An intrusion detection system". In Proceedings of the Fourth Aerospace Computer Security Applications Conference, pages 37-44, December 1988.
	C28	Snapp, "Signature Analysis and Communication Issues in a Distributed Intrusion Detection System," Master's Thesis, Department of Computer Science, University of California, Davis CA 95616, 1991.
	C29	Snapp et al., "DIDS (Distributed Intrusion Detection System) – Motivation, Architecture and An Early Prototype," Computer Security Laboratory, Division of Computer Science, Unic. Of California, Davis, Davis, CA.
	C30	Staniford-Chen, et al., "GrIDS- A Graph Based Intrusion Detection System for Large Networks," Proceedings of the 19th National Information Systems Security Conference, Volume 1, pp 361-370, October 1996.
	C31	Tener, "Discovery: An Expert System in the Commercial Data Security Environment", Fourth IFIP Symposium on Information Systems Security, Monte Carlo, December 1986.
	C32	Tener, "AI and 4GL: Automated Detection and Investigation Tools", Proceedings of the IFIP Sec. '88, Australia, 1989, pp 23-29.
	C33	Teng et al., "Adaptive Real-Time Anomaly Detection Using Inductively Generated Sequential Patterns," © 1990
	C34	Vaccaro et al., "Detection of Anomalous Computer Session Activity," © 1989 IEEE
	C35	Valdes, et al., "Adaptive, Model-based Monitoring for Cyber Attack Detection," Proceedings of Recent Advances in Intrusion Detection 2000 (RAID 2000), H. Debar, L. Me, F. Wu (Eds), Toulouse, France, Springer-Verlag LNCS Volume 1907, pp 80-92, October 2000.
	C36	Valdes, A., "Blue Sensors, Sensor Correlation, and Alert Fusion, http://www.raid-symposium.org/raid2000/Materials/Abstracts/41/avaldes_raidB.pdf, October 4, 2000
	C37	Valdes, et al., "Statistical Methods for Computer Usage Anomaly Detection Using NIDES (Next-Generation Intrusion Detection Expert System)," 3rd International Workshop on Rough Sets and Soft Computing, San Jose CA 1995, 306-311
	C38	Weiss, "Analysis of Audit and Protocol Data using Methods from Artificial Intelligence," Siemens AG, Munich, West Germany
	C39	Wimer, S., "The Core of CylantSecure," White Papers, http://www.cylant.com/products/core.html, Date Unknown, Alleged © 1999-2003 Cylant Inc., pgs 1-4
	C40	Winkler, "A UNIX Prototype for Intrusion and Anomaly Detection in Secure Networks," © Planning Research Corp. 1990

U.S. Department of Commerce, Patent and Trademark Office	Docket No.	Serial No.
(PTO-1449 modified)	SRI/4190-3	09/711,323
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Applicant de Jesus Valdes, et al.	Confirmation No.: 6879
(Use several sheets if necessary)	Filing Date	Group
Examiner	November 9, 2000	2161

	C41	Zhang, et al., "A Hierarchical Anomaly Network Intrusion Detection System using Neural Network Classification," Proceedings of the 2001 WSES International Conference on Neural Networks and Applications (NNA'01), Puerto de la Cruz, Canary Islands, Spain, February 11-15 2001.
Examiner		Date Considered 4/9/04

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with your communication to applicant.